



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/645,028	08/23/2000	Chris Rygaard	1010722-991101	1587

26379 7590 12/31/2003

GRAY CARY WARE & FREIDENRICH LLP
2000 UNIVERSITY AVENUE
E. PALO ALTO, CA 94303-2248

EXAMINER

JACKSON, JENISE E

ART UNIT

PAPER NUMBER

2131

DATE MAILED: 12/31/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

PATENT DOCKET	
DATE:	<u>Jan 5, 2004</u>
ACTION:	<u>Resp to OA</u>
DUE:	<u>31 March 2004</u>
DEAD:	<u>30 June 2004</u>

RECEIVED

JAN 5 2004

GRAY CARY
WARE & FREIDENRICH

Office Action Summary

Application No.

09/645,028

Applicant(s)

RYGAARD ET AL

Examiner

Jenise E Jackson

Art Unit

2131

- The MAILING DATE of this communication appears on the cover sheet with the correspondence address -

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☐ Responsive to communication(s) filed on ____.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-20 is/are pending in the application.
- 4a) Of the above claim(s) ____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) ____ is/are allowed.
- 6) ☒ Claim(s) 1-20 is/are rejected.
- 7) ☐ Claim(s) ____ is/are objected to.
- 8) ☐ Claim(s) ____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on ____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- 11) ☐ The proposed drawing correction filed on ____ is: a) ☐ approved b) ☐ disapproved by the Examiner.
- If approved, corrected drawings are required in reply to this Office action.
- 12) ☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

- 13) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. ____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.
- 14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).
- a) ☐ The translation of the foreign language provisional application has been received.
- 15) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) 95-b
- 4) ☐ Interview Summary (PTO-413) Paper No(s). ____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other.

DETAILED ACTION

Minor Deficiencies

As per paper number 6, submitted April 25, 2002, the US patent's that are included in paper number 6, are not cited on form 1449. Therefore, the Applicant should provide a 1449 that includes the US patents that were provided in paper 6 so that the patents can be considered.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

Claims 1-20 rejected under 35 U.S.C. 102(a) as being anticipated by Jansen et al. NIST Special Publication 800-19 – Mobile Agent Security (hereafter Jansen).

1. As per claims 1, 4, 6, 8, 11, Jansen teaches a mobile application (MA) security system (title, pg. 2 and section 3.2, bottom paragraph on page 9), comprising; one or more hosts connected to the server computer, each computer executing the mobile application that jumps between the hosts during execution(see pg. 2, pg. 17, section 4.1.4, 4.1.5), central computer for controlling the security of a MA(pg. 18-19 section 4.2 Protecting Agents); the central computer comprising means for monitoring the security of the MA as it jumps between hosts computers wherein the MA is communicated from a first host to a second host(see pg. 18-19 section 4.2 protecting agents), wherein the security monitoring means further comprises means for detecting

unwanted changes in the code associated with the MA when the MA is jumping between hosts (see pg. 6-7, section 2.3.4, pg. 10-11, section 3.3).

2. As per claim 2, Jansen teaches wherein the detecting means further comprises means for storing a copy of each MA when the MA first passes thorough the server, means for receiving the MA after it is executed by another host, and means for comparing the code of the MA after it is executed by another host, to the stored copy of the MA to determine if changes have been made to the code of the MA (Section 3.2, 3.3, pgs 9-11, section 4.2.2 Mutual Itinerary Recording teaches tracking and comparing the Itinerary list as it traverses the peers – Since Jansen discloses both central and distributed Central computer (see claim 1 above), this reads on using one stored copy for comparison purposes. Further to this point are the lists/tables, bottom list on page 14 and top list on page 19, which disclose many possible countermeasure means – one skilled in the art would provide for a one-to-one code compare at a minimum).

3. As per claim 3, Jansen teaches claim 1 wherein the detecting means further includes means for computing a checksum of the MA when the MA first passes through the server (pg. 19-20, teach Public Key and PRAC which are “cryptographic checksums” and are checked for accuracy. Each reads on “checksum”), means for receiving the MA after it is executed by another host, means for comparing the checksum of the mobile application (page 17, Path Histories teaches adding a signed entry to the path which is used to verify validity of the MA/message) after it is executed by another host to the stored checksum of the mobile application to determine if changes have been made to the code of the mobile application(see section 2.3.4 pg. 6-7, section 3.2, 3.3. pg. 9-12, and pg. 16, Signed Code section teaches digital

signature/Authenticode which provides "code signing" to provide means for determining an authentic message or not).

4. *With further regard to claim 4*, Jansen teaches security monitoring means comprises preventing a host from transmitting hostile code in a MA to another host (pgs 9-10, section 3.2, pg. 18-19, section 4.2, pg. 19 top paragraph teaches IBM Aglets prevent receiving platform from accepting agents from an agent platform not defined as a trusted peer).

5. As per **claims 5**, wherein preventing means comprises determining if the host dispatching the mobile application is trusted (pages 18-19, Protecting Agents, teaches trusted peers via IBM Aglets and Claim 3 above teaches Signed Code which infers trust), means for saving the code of the MA and means, when requested by another node, for providing the code for the MA to the requesting node (page 13-14, Protecting Agent Platform section – broadly discloses "trusted communications for MA's" which inherently includes requesting of MA and transmission of MA), means for stripping the code from an initially received MA if the host is not trusted(see pgs. 18-19, section 4.2). The Examiner asserts that Jansen teaches stripping code, because Jansen teaches identifying a non-trusted machine (see previous claim rejections) and hence many options exist as to how to stay safe from said machine, i.e. do not communicate with it, only transmit to it, attempt to re-verify that it is a trusted machine, only communicate with certain machines, strip code.

6. *With further regard to claim 6*, Jansen teaches security monitoring means comprises detecting unwanted changes in the state of the MA (page 17, State Appraisal teaches prevention of state corruption/modification).

7. As per **claim 7**, Jansen teaches claim 6/15 wherein the detecting means further comprises means for saving a copy of the state of a MA received from a node that received the MA, means for receiving data about the same MA after a jump to another node and means for comparing the state of the MA after the jump to another node with the stored state of the MA to ensure that the state of the MA has not changed (page 17, section 4.1.4, 4.1.5).
8. *With further regard to claim 8*, Jansen teaches security monitoring means comprises detecting unwanted changes to the itinerary of the MA (page 21, Section 4.2.2, pg. 22-23, section 4.2.4).
9. As per **claim 9**, Jansen teaches wherein the detecting means further comprises means for saving a copy of the itinerary of a MA received from a node that received the MA, means for receiving the same MA after a jump to another node and means for comparing the itinerary of the MA after the jump to another node with the stored itinerary of the MA to ensure that the itinerary of the MA has not changed (page 21-22, section 4.2.2, 4.2.3).
10. As per **claim 10**, Jansen teaches claim 8 wherein the itinerary comprises past historical itinerary data (page 17, Path Histories section AND page 21, Mutual Itinerary Recording and Itinerary Recording with Replication/Voting sections).
11. *With further regard to claim 11*, Jansen teaches receiving data about a mobile application via State Appraisal, Path Histories, Proof Carrying Code (pages 16-18), which provides data about the MA (and reads on the claim).
12. As per **claim 12**, rejected under the same basis as claim 2.
13. With further regard to **claim 13**, see claim 1, 4 and 11 rejections above.
14. As per **claim 14**, it is rejected under the same basis as claim 5.

Art Unit: 2131

15. With further regard to **claim 15**, see claim 1, 6 and 11 rejections above.
16. As per **claim 16**, it is rejected under the same basis as per claim 7.
17. With further regard to **claim 17**, see claim 1, 8 and 11 rejections above.
18. As per **claim 18**, it is rejected under the same basis as claim 9.
19. As per **claim 19**, it is rejected under the same basis as per claim 10.
20. With further regard to **claim 20**, see claim 1, 4 and 11 rejections above (note that a non-trusted host launching a MA reads on hostile code, as per claim 4 and is disclosed in Jansen).

Double Patenting

21. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and, *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent is shown to be commonly owned with this application. See 37 CFR 1.130(b).

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

22. Claims 1-20 are rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1-20 of U.S. Patent No. 09/764548. Although the conflicting claims are not identical, they are not patentably distinct from each other(see below for explanation).

23. As per claim 1 of instant application 09/645028, and as per claim 1 of 09/764548, application 09/645028 discloses one or more hosts, and application 09/764548 discloses one or more nodes. It would have been obvious to one of ordinary skill at the time of the invention to modify one or more host with one or more nodes; the motivation is that a node is a device that can communicate with other network devices.

24. As per claim 1, of instant application 09/645028, and as per claim 1 of 09/764548, application 09/645028 discloses a mobile application security system, comprising: one or more host computers connected to the server computer, each host computer executing the mobile application that jumps between the hosts during execution, and application 09/764548 discloses, one or more nodes of a peer-to-peer network wherein each node is configured to execute a mobile application. As per the limitations of nodes it has already been addressed above.

25. It would have been obvious to modify computer connected to the server computer with a peer-to-peer network, the motivation is that a hosts computer connected to a server, is a peer-to-peer network because hosts and server distribute and receive information between each other on the network.

26. It would have been obvious to modify executing the mobile application that jumps between the hosts during execution, with wherein each node is configured to execute a mobile

Art Unit: 2131

application, the motivation is that a node must execute a mobile application before, the mobile application jumps to another hosts.

27. The Examiner asserts that the central computer of instant application 09/645028, is inherent to the central security enforcement node of application 09/764548, because the central computer, enforces security by monitoring the mobile applications.

28. All other limitations of claim 1 of instant application 09/645028, and 09/764548 recite same limitations.

29. As per claim 2 of instant application 09/645028, and as per claim 2 of 09/764548, application 09/645028 discloses first passes through the server, and application 09/764548 discloses is created by having the creating node send a copy of the mobile application to the central security enforcement node(CSEN). It would have been obvious to one of ordinary skill in the art to modify first passes through the server with is created by having the creating node send a copy of the mobile application to the central security enforcement node, the motivation is that one must first create a mobile application and send a copy to the CSEN, because the CSEN monitors the security between nodes, and it cannot be passed to the server until it is created.

30. As per claim 2 of instant application 09/645028, and as per claim 2 of 09/764548, application 09/645028 discloses receiving the mobile application, and application 09/764548 discloses receiving data about the mobile application. It would have been obvious to modify receiving the mobile application with receiving data about the mobile application; the motivation is that data is received from a mobile application, because the mobile application is executed.

31. As per claim 2 of instant application 09/645028, and as per claim 2 of 09/764548, application 09/645028 discloses after it is executed, and application 09/764548 discloses when it

is received. It would have been obvious to one of ordinary skill in the art at the time of the invention to modify after it is executed with when it is received, the motivation is that the mobile application must first be executed before it is received by another host(i.e. node), because mobile application are executed on each node before being passed to another host.

32. All other limitations as per claim 2 of instant application 09/645028, and as per claim 2 of 09/764548 recite same limitations.

33. As per claim 3 of instant application 09/645028, and as per claim 3 of 09/764548, application 09/645028 discloses computing a checksum, and 09/764548 discloses for receiving a checksum. It would have been obvious to one of ordinary skill in the art at the time of the invention to modify computing a checksum with receiving a checksum; the motivation is that the checksum must first be received in order to compute the checksum.

34. As per claim 3 of instant application 09/645028, and as per claim 3 of 09/764548, application 09/645028 discloses after it is executed, and 09/764548 discloses after it is sent. It would have been obvious to one of ordinary skill in the art at the time of the invention to modify after it is executed with after it is sent; the motivation is that one must execute the mobile application before it is sent to another node.

35. As per claim 3 of instant application 09/645028, and as per claim 3 of 09/764548, the limitations of is created, and after it is received as already been addressed same motivation applies as above(see claim 2).

36. All other limitations as per claim 3 of instant application 09/645028, and as per claim 3 of 09/764548 recite same limitations.

Art Unit: 2131

37. As per claim 4 of instant application 09/645028, and as per claim 4 of 09/764548, recites same limitations as per claim 1 above. Same motivation applies to limitations(see claim 1 above). All other limitations as per claim 4 of instant application 09/645028, and as per claim 4 of 09/764548, recites same limitations.

38. As per claim 5 of instant application 09/645028, and as per claim 5 of 09/764548 recite same limitations. As per limitation of node it has already been addressed same motivation applies(see claim 1 above).

39. As per claim 6 of instant application 09/645028, and as per claim 6 of 09/764548, recites same limitations as per claim 1 above. Same motivation applies to limitations (see claim 1 above). All other limitations as per claim 6 of instant application 09/645028, and as per claim 6 of 09/764548, recites same limitations.

40. As per claim 7 of instant application 09/645028, and as per claim 7 of 09/764548, recites same limitations.

41. As per claim 8 of instant application 09/645028, and as per claim 8 of 09/764548, recites same limitations as per claim 1 above. Same motivation applies to limitations (see claim 1 above). All other limitations as per claim 8 of instant application 09/645028, and as per claim 8 of 09/764548, recites same limitations.

42. As per claim 9 of instant application 09/645028, and as per claim 9 of 09/764548, recites same limitations.

43. As per claim 10 of instant application 09/645028, and as per claim 10 of 09/764548, recites same limitations.

44. As per claim 11 of instant application 09/645028, and as per claim 11 of 09/764548, recites limitations of central security enforcement node, and peer-to-peer network has already been addressed(see claim 1). Same motivation applies above(see claim 1). As per the limitation of data it has already been addressed(see claim 2 above), same motivation applies above.

All other limitations as per claim 11 of instant application 09/645028, and as per claim 11 of 09/764548, recites same limitations.

45. As per claim 12 of instant application 09/645028, and as per claim 12 of 09/764548, the limitations of created and received has already been addressed(see claim 3). Same motivation applies above(see claim 3). All other limitations as per claim 12 of instant application 09/645028, and as per claim 12 of 09/764548, recites same limitations.

46. As per claim 13 of instant application 09/645028, and as per claim 13 of 09/764548, the limitations of central security enforcement node, and peer-to-peer network has already been addressed(see claim 1). Same motivation applies above(see claim 1). As per the limitation of data it has already been addressed(see claim 2 above), same motivation applies above.

47. As per claim 14 of instant application 09/645028, and as per claim 14 of 09/764548, application 09/645028 discloses stripping the code from an initially received mobile application, and 09/764548 discloses stripping the code from a mobile application. It would have been obvious to modify stripping the code from an initially received mobile application with stripping the code from a mobile application, the motivation is that the mobile application has to be received otherwise the code cannot be stripped.

48. As per claim 15 of instant application 09/645028, and as per claim 15 of 09/764548, the limitations of central security enforcement node, and peer-to-peer network has already been

addressed(see claim 1). Same motivation applies above(see claim 1). As per the limitation of data it has already been addressed(see claim 2 above), same motivation applies above.

49. As per claim 16 of instant application 09/645028, and as per claim 16 of 09/764548, the limitation of a data has already been addressed(see claim 2 above), same motivation applies above. All other limitations as per claim 16 of instant application 09/645028, and as per claim 16 of 09/764548, recites same limitations.

50. As per claim 17 of instant application 09/645028, and as per claim 17 of 09/764548, the limitations of central security enforcement node, and peer-to-peer network has already been addressed(see claim 1). Same motivation applies above(see claim 1). As per the limitation of data it has already been addressed(see claim 2 above), same motivation applies above.

51. As per claim 18 of instant application 09/645028, and as per claim 18 of 09/764548, the limitation of a node as already been addressed(see claim 1), same motivation applies above(claim 1). Also, the limitation of data has already been addressed see claim 2, same motivation applies above.

52. As per claim 19 of instant application 09/645028, and as per claim 19 of 09/764548, recites same limitations.

53. As per claim 20 of instant application 09/645028, and as per claim 20 of 09/764548, the limitations of central security enforcement node, and peer-to-peer network has already been addressed(see claim 1). Same motivation applies above(see claim 1). As per the limitation of data, it has already been addressed(see claim 2 above), same motivation applies above.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jenise E Jackson whose telephone number is (703) 306-0426.


The examiner can normally be reached on M-Th (6:00 a.m. - 3:30 p.m.) alternate Friday's.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (703) 305-9648. The fax phone numbers for the organization where this application or proceeding is assigned are (703) 305-0040 for regular communications and (703) 308-6306 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.



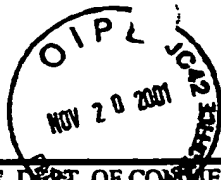
December 18, 2003


EMMANUELL L. MOISE
PRIMARY EXAMINER

Application/Control Number: 09/645,028

Art Unit: 2131

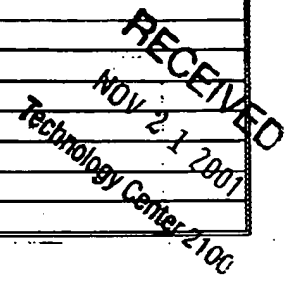
Page 14



Form PTO-1449 U.S. DEPT. OF COMMERCE (modified 2/91) Patent and Trademark Office INFORMATION DISCLOSURE CITATION (Use several sheets if necessary)	Attorney Docket Number: 1010722-991101	Serial Number: 09/645,028
	Applicant: Chris Rygaard	
	Filing date: 23 August 2000	Group art unit:

U.S. PATENT DOCUMENTS

Examiner Initial	Patent Number	Date	Name	Class	Sub-class	Filing date if appropriate



FOREIGN PATENT DOCUMENTS

Document number	Date	Country	Class	Sub-class	Translation
					YES NO

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

88	Peter Mell et al., "A Denial of Service Resistant Intrusion Detection Architecture", NIST, 2000
	Peter Mell et al., "Mobile Agent Attach Resistant Distributed Hierarchical Intrusion Detection" NIST, 1999
	W.A. Jansen, "A Privilege Management Scheme for Mobile Agent Systems", NIST
	Wayne Jansen, "Countermeasures for Mobile Agent Security", NIST
	Wayne Janson et al., "Applying Mobile Agents to Intrusion Detection and Response" NIST Interim Report, October 1999
	Wayne Janson et al., "Privilege Management of Mobile Agents", NIST
1 80	Wayne Jansen et al., "NIST Special Publication 800-19 - Mobile Agent Security", NIST

Examiner: <i>Jenise Jacobs</i>	Date Considered: <i>12/17/03</i>
EXAMINER: Initial if citation considered, whether or not citation is in conformance with MPEP '609; Draw line through if not in conformance and not considered. Include copy of this form with next communication to the applicant.	

74

Notice of References Cited	Application/Control No. 09/645,028	Applicant(s)/Patent Under Reexamination RYGAARD ET AL.	
	Examiner Jenise E Jackson	Art Unit 2131	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
	A	US-6,009,456	12-1999	Frew et al.	709/202
	B	US-6,148,327	11-2000	Whitebread et al.	709/202
	C	US-6,615,232	09-2003	Suzuki et al.	709/202
	D	US-6,622,157	09-2003	Heddaya et al.	709/202
	E	US-6,192,354	02-2001	Bigus et al.	706/46
	F	US-5,974,549	10-1999	Golan, Gilad	713/200
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.